DETAILED ACTION

1. Claims 1-7 and 10-19 are pending in this office action.

2. Applicant's arguments, filed August 15, 2008, have been fully considered but they are not persuasive.

Claim Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-7 and 10-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al. (Handbook of Applied Cryptography, 1997, section 13.3.1, pages 551-553) in view of Weiant, Jr. et al. (U.S. Patent No. 6,044,350).

Regarding claim 1, Menezes et al. teaches an asymmetric cryptographic processing system using a multiple key hierarchy, the asymmetric cryptographic processing system comprising:

- A first key for performing asymmetric operations at a first rate, wherein each operation requires a first cryptographic processing time (page 552, step 3, *data*

keys, provide cryptographic operations on user data, tend to be short-term keys); and

- A second key for performing an asymmetric cryptographic processing operation to update the first key (page 552, step 2, *key-encrypting keys*), wherein the second key is used for cryptographic processing operations for the first key at a second rate that is less often than the first rate (page 552, step 2, *key-encrypting keys*, the key-encrypting keys are used less often than the keys that they encrypt).

Menezes et al. does not specifically teach the second key requires a second cryptographic processing time greater than the first cryptographic processing time.

Weiant, Jr. et al. teaches the second key requires a second cryptographic processing time greater than the first cryptographic processing time (fig. 3).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the second key requiring more processing time than the first key, as taught by Weiant, Jr. et al., with the method/medium of Menezes et al. It would have been obvious for such modifications because longer length keys take more time to process, in order to provide more security, with a tradeoff that the key does not have to be replaced as often.

Regarding claims 2-5, Menezes et al. as modified by Weiant, Jr. et al. teaches wherein the system is used to cryptographically process and transfer digital [voice/audio/video] data in a network (see col. 3, lines 32-38 of Weiant, Jr. et al.).

Regarding claim 6, Menezes et al. as modified by Weiant, Jr. et al. teaches wherein the second key is hard coded into the system at the time of manufacturing the system (see page 551, section 13.3.1, step 1 of Menezes et al.).

Regarding claim 7, Menezes et al. as modified by Weiant, Jr. et al. teaches wherein a plurality of digital cryptographic processing systems are coupled by a telecommunications system, wherein the second key is distributed to two or more of the asymmetric cryptographic processing systems via the telecommunications system (see fig. 2 of Weiant, Jr. et al.).

Regarding claim 10, Menezes et al. as modified by Weiant, Jr. et al. teaches a method for providing secure data transactions in a telecommunications system, wherein a digital processing device receives information from the telecommunications system (see fig. 2, ref. num 234 of Weiant, Jr. et al.), wherein the digital processing device uses a first asymmetrical cryptographically processed key to perform an asymmetric cryptographic processing operation to decode the information wherein the cryptographic processing operation is at a first level of complexity requiring a first amount of resources by the processing device (see page 552, step 3, *data keys* of Menezes et al.), wherein

the cryptographic processing operation is performed at a first rate of cryptographic processing operations per unit time (see page 552, step 3, *data keys* of Menezes et al., provide cryptographic operations on user data, tend to be short-term keys), the method comprising:

- Transferring a second asymmetrical cryptographically processed key to the digital processing device, wherein the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity requiring a second amount of resources by the processing device that is higher than the first amount of resources (see page 552, step 3, *data keys* of Menezes et al., the data keys are used, perhaps for every type of data they encrypt);
- Updating the first asymmetrical cryptographically processed key from time-to-time (see page 552, step 3 of Menezes et al.), wherein the updating of the first asymmetrical cryptographically processed key occurs at a second rate of cryptographic processing operations per unit time that is less than the first rate of cryptographic processing operations per unit time (see fig. 3, key B of Weiant, Jr. et al.), wherein the updating includes the following substeps:
    - Encoding a substitute first asymmetrical cryptographically processed key with a second key, so that the resulting cryptographically processed substitute first asymmetrical cryptographically processed key is decodable by the second asymmetrical cryptographically processed key (see page

552, paragraph below step 3 of Menezes et al., keys at one layer are used to protect items at a lower level); and

- Transferring the substitute first asymmetrical cryptographically processed key to the digital processing device so that the substitute first asymmetrical cryptographically processed key is used in subsequent cryptographic processing operations by the digital processing device (see fig. 2, ref. num 234 of Weiant, Jr. et al.).

Regarding claim 11, Menezes et al. as modified by Weiant, Jr. et al. teaches further comprising:

- Transferring a third asymmetrical cryptographically processed key to the digital processing device (see page 551, section 13.3.1, step 1, master key of Menezes et al.), wherein the third asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a third level of complexity requiring a third amount of resources by the processing device that is higher than the second amount of resources (see page 551, section 13.3.1, step 1 of Menezes et al. and fig. 3, key C of Weiant, Jr. et al.);
- Updating the second asymmetrical cryptographically processed key from time-to-time (see page 552, step 2 of Menezes et al.), wherein the updating of the second asymmetrical cryptographically processed key occurs at a third rate of cryptographic processing operations per unit time that is less than the second

rate of cryptographic processing operations per unit time (see fig. 3, key C of Weiant, Jr. et al.), wherein the updating includes the following substeps:

- Encoding a substitute second asymmetrical cryptographically processed key with a third asymmetrical cryptographically processed key, so that the resulting cryptographically processed substitute second asymmetrical cryptographically processed key is capable of being cryptographically processed by the third asymmetrical cryptographically processed key (see page 552, paragraph below step 3 of Menezes et al., keys at one layer are used to protect items at a lower level); and
- Transferring the substitute second asymmetrical cryptographically processed key to the digital processing device so that the substitute second asymmetrical cryptographically processed key is used in subsequent cryptographic processing operations by the digital processing device (see fig. 2, ref. num 234 of Weiant, Jr. et al.).

Regarding claims 12-15, the examiner takes Official Notice that the resources include [processing time/transistor density on an IC/memory capacity/data bandwidth] because these resources are well-known tradeoffs of resource intensive actions as cryptography.

Claims 16-19 rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al. (U.S. Patent No. 5,850,443) in view of Davis (U.S. Patent No. 5,796,840).

Regarding claim 16, Van Oorschot et al. teaches a method of updating a cryptographic key used for decrypting distributed data, the method comprising:

- Generating a first key for decrypting the distributed data, the first key of a first length (col. 6, lines 25-29);
- Encrypting the first key with a second key, the second key of a second length, wherein the second length is longer than the first length (col. 6, lines 29-31); and
- Distributing the encrypted first key (fig. 1 and col. 6, lines 31-33).

Van Oorschot et al. does not teach wherein the first key updates the cryptographic key; and wherein the cryptographic key, the first key, and the second key encrypt and decrypt data using a similar class of algorithm to encrypt and decrypt data.

Davis teaches wherein the first key updates the cryptographic key (col. 6, lines 7-27); and wherein the cryptographic key, the first key, and the second key encrypt and decrypt data using a similar class of algorithm to encrypt and decrypt data (fig. 7, all use asymmetric key for encryption and decryption).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine updating the cryptographic key with the first key and all keys are from a similar class of algorithm, as taught by Davis, with the method of Van Oorschot et al. It would have been obvious for such modifications because the systems involved would only have to be programmed to handle one type of cryptographic algorithm.

Regarding claim 17, Van Oorschot et al. as modified by Davis teaches further comprising distributing data encrypted with the first key (see fig. 2 of Van Oorschot et al.).

Regarding claim 18, Van Oorschot et al. as modified by Davis teaches further comprising:

- Generating a third key to replace the first key, the third key of a third length, wherein the third length is shorter than the second length (see col. 6, lines 46-49 of Van Oorschot et al.);
- Encrypting the third key with the second key (see col. 6, lines 43-46 of Van Oorschot et al.); and
- Distributing the encrypted third key (see fig. 3 of Van Oorschot et al.).

Regarding claim 19, Van Oorschot et al. as modified by Davis teaches further comprising distributing data encrypted with the third key (see fig. 4 of Van Oorschot et al.).

Response to Arguments

5. Applicant argues:

a. Menezes and Weiant, Jr. et al. do not teach a first key for performing asymmetric operations at a first rate, a second key for updating the first key, and the second key is at a second rate that is less often than the first rate (page 7 and 8).

b. Van Oorschot et al. and Davis do not teach where the distributed first key updates the cryptographic key (page 9).

Regarding argument (a), examiner disagrees. Menezes teaches two keys, one which changes at a first rate (data key); the second key changes at a second rate (key-encrypting key). The first key gets used more often because it is used for encrypting data. The second key gets used less often because is used for updating/changing keys. As is obvious in the art, a key that encrypts data is used at a higher rate than a key that is used for key changes/updates.

Regarding argument (b), examiner disagrees. Claim 16 was a 103, combination rejection between Van Oorschot et al. and Davis. Davis alone may not teach a distributed first key, as argued by applicant, but the combination of Van Oorschot et al.

and Davis teaches a distributed key, wherein the key is used for updating a cryptographic key.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON S. HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon S Hoffman/
Primary Examiner, Art Unit 2436